सत्याला मरण नाही

ALL INDIA SHRI SHIVAJI MEMORIAL SOCIETY'S
INSTITUTE OF INFORMATION TECHNOLGY

Department Of
Information Technogy
PRESENTS...

Unplugged

Annual Technical Magzine
2015

Designed By: Rishikesh Jadhav

DEPARTMENT OF INFORMATION TECHNOLOGY

Welcome to the department of Information Technology.

As we all know, this is an era of Information Technology, and almost every one of us uses some device or a gadget which invariably leverages the benefits of Information Technology. The advent of Information Technology has revolutionized the way we live. Moreover Internet and mobile wireless technology are the boons of Information Technology. So, the department strives hard to groom our students with this cutting edge technology, thereby instilling high valued ethics and morale. The department prepares them to take up the challenges of ever changing dynamic IT industry.

To fulfill the vision and mission of Information Technology Department towards imparting quality education to our students we conduct various activities like expert lectures, seminar and workshops and industrial visit to make teaching process effective. We provide a platform to our students to participate in many extra-curricular activities through various technical, non-technical contests for their overall personality development.

Message from HOD

It gives me an immense pleasure and pride that Department of Information Technology is publishing 3rd annual technical magazine "UNPLUGGED – 2015". It is the presentation of student's hidden talent and caliber. It is the platform of and by our students for gathering, sharing and presenting creative ideas.

This technical magazine is a collection of technical papers, articles etc. which will be the hub for the students and readers to broadcast and enhance their knowledge.

Finally, I express my sincere gratitude and thanks to Hon'ble Shri Malojiraje Chhatrapati– Honorary Secretary of All India Shri Shivaji Memorial Society and Dr. P. B. Mane – Principal AISSMS IOIT for their valuable guidance and support.

I thank the chief editor Mrs. Reshma Y. Totare and her team of staff and students editors for providing students the area for creative thoughts and knowledge expansion.

Prof. Pritesh A. Patil
HOD, I.T Department
AISSMS IOIT, Pune

Message from EDITOR

It gives me an immense pleasure as our Department of Information Technology is presenting 3rd annual technical magazine "UNPLUGGED – 2015" to our dear reader.

"UNPLUGGED" providing a technical platform to the students and teachers to express their innovative ideas, hidden talent and writing skills.

I am very thankful to Hon'ble Shri Malojiraje Chhatrapati – Honorary Secretary of All India Shri Shivaji Memorial Society and Principal, Dr. P. B. Mane. I must thank our Head of Department, Prof. Pritesh A. Patil for his continuous encouragement and guidance and also for giving me the opportunity to work as the editor of magazine. Special thanks to the entire enthusiastic participant as without their contribution this magazine would not have been possible. There is equal contribution of student editor team to make this difficult task possible.

I am sure you will enjoy reading the interesting articles in the magazine.

Mrs. Reshma Yogesh Totare
Chief Editor and Magazine Coordinator
Assistant Professor
Department of Information Technology

Editorial Team – Unplugged 2015

[L-R]: **Sagar Soni**
Rishikesh Jadhav
Mrunal Datar
Shruti Bhagwat

LINUX KERNELS

[Tux the penguin, mascot of Linux]

The **Linux kernel** is a Unix-like computer operating system kernel. The Linux kernel is a widely used operating system kernel world-wide; the Linux operating system is based on it and deployed on both traditional computer systems, usually in the form of Linux distributions, and on embedded devices such as routers. The Android operating system for tablet computers and smartphones is also based atop the Linux kernel.

The Linux kernel API, the application programming interface (API) through which user programs interact with the kernel, is meant to be very stable and to not break userspace programs (some programs, such as those with GUIs, rely on other APIs as well). As part of the kernel's functionality, device drivers control the hardware; "mainlined" device drivers are also meant to be very stable. However, the interface between the kernel and loadable kernel modules (LKMs), unlike in many other kernels and operating systems, is not meant to be very stable by design.

The Linux kernel, developed by contributors worldwide, is a prominent example of free and open source software. Day-to-day development discussions take place on the Linux kernel mailing list (LKML). The Linux kernel is released under the GNU General Public License version 2 (GPLv2), with some firmware images released under various non-free licenses.

In April 1991, Linus Torvalds, a 21-year-old student at the University of Helsinki Finland started working on some simple ideas for an operating system. He started with a task switcher in Intel 80386 assembly language and a terminal driver. On 25 August 1991, Torvalds posted the following to *comp.os.minix*, a newsgroup on Usenet.

After that, many people contributed code to the project. Early on, the MINIX community contributed code and ideas to the Linux kernel. At the time, the GNU Project had created many

of the components required for a free operating system, but its own kernel, GNU Hurd, was incomplete and unavailable. The BSD operating system had not yet freed itself from legal encumbrances. Despite the limited functionality of the early versions, Linux rapidly accumulated developers and users.

A newsgroup known as *alt.os.linux* was started, and on 19 January 1992, the first post to alt.os.linux was made. On 31 March 1992, alt.os.linux became *comp.os.linux*.

VERSION HISTORY

The X Window System was soon ported to Linux. In March 1992, Linux version 0.95 was the first to be capable of running X. This large version number jump (from 0.1x to 0.9x) was due to a feeling that a version 1.0 with no major missing pieces was imminent. However, this proved to be somewhat overoptimistic, and from 1993 to early 1994, 15 development versions of version 0.99 appeared.

On 14 March 1994, Linux 1.0.0 was released, with 176,250 lines of code. In March 1995, Linux 1.2.0 was released (310,950 lines of code).

Version 2 of Linux, released on 9 June 1996, was followed by additional major versions under the version 2 header:

- 25 January 1999 - Linux 2.2.0 was released (1,800,847 lines of code).
- 18 December 1999 - IBM mainframe patches for 2.2.13 were published, allowing Linux to be used on enterprise-class machines.
- 4 January 2001 - Linux 2.4.0 was released (3,377,902 lines of code).
- 17 December 2003 - Linux 2.6.0 was released (5,929,913 lines of code).

Starting in 2004, the release process changed and new kernels started coming out on a regular schedule every 2–3 months, numbered 2.6.0, 2.6.1, up through 2.6.39.

On 21 July 2011 Linus Torvalds announced the release of Linux 3.0: "Gone are the 2.6 <bignum> days". The version bump is not about major technological changes when compared to Linux 2.6.39; it marks the kernel's 20th anniversary. The time-based release process remained the same.

As of 2013, the Linux 3.10 release had 15,803,499 lines of code.

CURRENT VERSION

Currently, Linux is licensed only under version 2 of the GPL, without offering the licensee the option to choose "any later version", and there is some debate over how easily it could be changed to use later GPL versions such as version 3 (and whether this is even

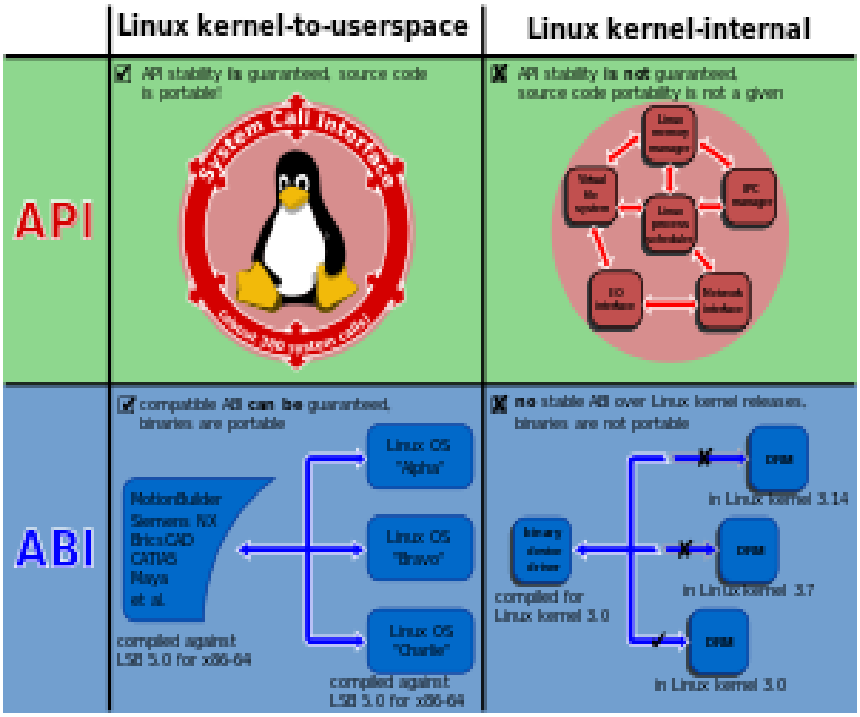
desirable).Torvalds himself specifically indicated upon the release of version 2.4.0 that his own code is only under version 2. However, the terms of the GPL state that if no version is specified, then any version may be used, and Alan Cox pointed out that very few other Linux contributors have specified a particular version of the GPL. In September 2006, a survey of 29 key kernel programmers indicated 28 preferred GPLv2 to the then-current GPLv3 draft.

Linux kernel is a monolithic kernel. Device drivers and kernel extensions run in kernel space, with full access to the hardware, although some exceptions run in user space, for example file systems based on FUSE. The graphics system most people use with Linux does not run within the kernel, in contrast to that found in Microsoft Windows. Unlike standard monolithic kernels, device drivers are easily configured as modules, and loaded or unloaded while running the system. Also unlike standard monolithic kernels, device drivers can be pre-empted under certain conditions. This latter feature was added to handle hardware interrupts correctly, and to improve support for symmetric multiprocessing. By choice, the Linux kernel has no Binary Kernel Interface.

The hardware is also incorporated into the file hierarchy. Device drivers interface to user applications via an entry in the /dev or /sys directories. Process information as well is mapped to the file system through the /proc directory.

Linux kernel supports true preemptive multitasking (both in user mode and kernel mode), virtual memory, shared libraries, demand loading, shared copy-on-write executables (via KSM), memory management, the Internet protocol suite, and threading.

PROGRAMMING LANGUAGE



The Linux kernel is written in the version of the C programming language supported by GCC (which has introduced a number of extensions and changes to standard C), together with a number of short sections of code written in the assembly language (in GCC's "AT&T-style" syntax) of the target architecture. Because of the extensions to C it supports, GCC was for a long time the only compiler capable of correctly building the Linux kernel.

SECURITY

Computer security is a much-publicized topic in relation to the Linux kernel, because a large portion of the kernel bugs can present potential security flaws as they may allow for privilege escalation or create denial-of-service attack vectors. Over the years, numerous such flaws were found and fixed in the Linux kernel. New security features are continuously implemented to address computer insecurity issues in the Linux kernel.

Critics have accused kernel developers of covering up security flaws or at least not announcing them. In response, in 2008, Linus Torvalds replied, "I personally consider security bugs to be just 'normal bugs'. I don't cover them up, but I also don't have any reason what-so-ever to think it's a good idea to track them and announce them as something special...one reason I refuse to bother with the whole security circus is that I think it glorifies—and thus encourages—the wrong behavior. It makes 'heroes' out of security people, as if the people who don't just fix normal bugs aren't as important. In fact, all the boring normal bugs are *way* more important, just because there's a lot more of them. I don't think some spectacular security hole should be glorified or cared about as being any more 'special' than a random spectacular crash due to bad locking."

At times, bugs have been corrected in Linux before other systems. In May 2012, a difference between the implementations of the SYSRET instruction in AMD and Intel processors was found to cause vulnerabilities in major systems such as Windows, FreeBSD, XenServer, and Solaris. The issue had been fixed in the Linux kernel since 2006.

Raw hardware devices are protected from direct access, and the file system has an inbuilt security system giving individual access to files on three levels, user only, group membership, and world access.

SAGAR SONI

TE – IT

THE NUANCES OF CLOUD ECONOMICS

ECONOMICS IS CENTRAL TO CLOUD COMPUTING.

The cloud's financial and strategic benefits have been the catalysts for its explosive growth, and pay-per-use pricing, sometimes referred to as measured service, 1 is a core attribute. Some say that cost reduction and business agility are the two most important benefits of the cloud,2 some argue that economies of scale from large providers are the main drivers of cloud benefits,3 and others therefore conclude that eventually all IT should and will move to the cloud.4 However, the theory and practice of cloud economics are considerably more nuanced, and encompass numerous challenges, ranging from the practical to the theoretical, across service architecture, statistics, behavioral economics, computing foundations, game theory, business strategy, and regulatory policy.

PRIVATE, PUBLIC, OR HYBRID SOME CONSIDER "PRIVATE CLOUD" TO BE A MISNOMER.

However, many of the key criteria of cloud still apply, such as dynamic allocation of resources from a common pool and pay-per-use pricing through either a commercial transaction or chargeback to an internal customer. A basic question facing most IT shops today is whether to use their own datacenters, a public cloud provider, colocation facilities, or all of the above. Organizations must consider many quantitative and qualitative criteria when making this decision, such as focusing leadership time on "core vs. context" issues—that is, those that are critical to developing competitive advantage versus those that aren't.5 For example, a movie studio should focus on scripting, cinematography, and casting, not datacenter technology and operations. From a rational economic cost-optimization perspective, however, there are several key drivers. The first driver is the loaded unit cost of a company's IT relative to the offered unit price of the cloud service provider. The cost structure for public cloud service providers might be better, but additional components can increase the offered price, such as a provider's profit, underutilized resources, taxes, and sales, general, and administrative expenses. If a company's IT shop is not cost-optimized or can't achieve scale and high utilization, the cloud might well offer a cost advantage, but for well-run organizations, the unit costs for public cloud services might actually be higher.

STATISTICAL MULTIPLEXING EFFECTS

To understand relative costs, you also can't just look at unit costs, but must also consider utilization. Operating, say, at 33 percent utilization means that there are two unused resources for every one that is used. The effective unit cost then triples, not unlike buying two additional peaches at the fruit stand for every one that you actually eat. In the case of the public cloud, this is factored into the offered price. In the case of dedicated resources, low utilization can be caused by poor resource management, but it can also be an inevitable result of spiky workloads in the presence of fixed capacity. Both public and private clouds create utilization benefits through workload aggregation. When workloads are statistically independent, multiplexing them smooth aggregate demand: the troughs and peaks tend to cancel each other out. As a result of this smoothing, both private and public clouds can achieve better resource utilization than if the workloads were individually run on soloed resources.

ON-DEMAND PROVISIONING

Having the right quantity of resources to match aggregate demand has clear economic benefits. Too many resources, and there is a loss commensurate with the opportunity cost of the capital deployed or excess expense. Too few, and the application will perform slowly or not at

all, impacting key metrics such as revenue (for customer-facing applications), labor productivity (for employee ones), or time to market—for example, for cloud-based collaboration among partners. On-demand resources ensure the right quantity at the right time.

HUMAN BEHAVIOR

Classical economics, in which individuals behave rationally and optimally, has been complemented, or perhaps even supplanted, by behavioral economics, in which humans often behave irrationally and emotionally.17 Cloud computing and enterprise IT aren't immune from such cognitive biases. Everything from "free-to-play" games, which have in-app purchases, to "free tiers" of use provide real-world examples of the application of such behavioral economic insights to business and cloud strategy.

ABRAR AHMED SHAIKH

TE-IT

MIND THE GAP: NANOSCALE SPEED BUMP COULD REGULATE PLASMONS FOR HIGH-SPEED DATA FLOW

The name sounds like something Marvin the Martian might have built, but the "nanomechanicalplasmonic phase modulator" is not a doomsday device. Developed by a team of government and university researchers, including physicists from the National Institute of Standards and Technology (NIST), the innovation harnesses tiny electron waves called plasmons. It's a step towards enabling computers to process information hundreds of times faster than today's machines.

Computers currently shuttle information around using electricity traveling down nanoscale metal wires. Although inexpensive and easy to miniaturize, metal wires are limited in terms of speed due to the resistance in the metal itself. Fiber optics use light to move information about 10,000 times faster, but these and other nonmetallic waveguides are constrained by pesky physical laws that require critical dimensions to be at least half the wavelength of the light in size; still small, but many times larger than the dimensions of current commercial nanoscale electronics.

Plasmonics combines the small size and manufacturability of electronics with the high speeds of optics. When light waves interact with electrons on a metal's surface, strong fields with dimensions far smaller than the wavelength of the original light can be created--plasmons. Unlike light, these plasmons are free to travel down nanoscale wires or gaps in metals.

The team, which included researchers from Rutgers, the University of Colorado at Colorado Springs, and Argonne National Laboratory, fabricated their device using commercial nanofabrication equipment at the NIST NanoFab. Small enough to serve in existing and future computer architectures, this technology may also enable electrically tunable and switchable thin optical components.

Their findings were published in *Nature Photonics*.

The plasmonic phase modulator is effectively an inverted, nanoscale speed bump. Eleven gold strands are stretched side by side like footbridges across a 23-micrometer gap just 270 nanometers above the gold surface below them. Incoming plasmons, created by laser light at one end of the array, travel though this air gap between the bridges and the bottom gold layer.

When a control voltage is applied, electrostatic attraction bends the gold strands downwards into a U shape. At a maximum voltage--close to the voltages used in today's computer chips--the gap narrows, slowing the plasmons. As the plasmons slow, their wavelength becomes shorter,

allowing more than an extra half of a plasmonic wave to fit under the bridge. Because it's exactly out of phase with the original wave, this additional half wavelength can be used to selectively cancel the wave, making the bridge an optical switch.

At 23 micrometers, the prototype is relatively large, but according to NIST researcher Vladimir Aksyuk, their calculations show that the device could be shortened by a factor of 10, scaling the device's footprint down by a factor of 100. According to these calculations, the modulation range can be maintained without increase in the optical loss, as the length and the size of the gap are reduced.

"With these prototypes, we showed that nanomechanical phase tuning is efficient," says Aksyuk. "This effect can be generalized to other tunable plasmonic devices that need to be made smaller. And as they get smaller, you can put more of them on the same chip, bringing them closer to practical realization."

SHAGUFTA SHAIKH

BE – IT

COMPUTERS THAT MIMIC THE FUNCTION OF THE BRAIN

Researchers are always searching for improved technologies, but the most efficient computer possible already exists. It can learn and adapt without needing to be programmed or updated. It has nearly limitless memory, is difficult to crash, and works at extremely fast speeds. It's not a Mac or a PC; it's the human brain. And scientists around the world want to mimic its abilities.

Both academic and industrial laboratories are working to develop computers that operate more like the human brain. Instead of operating like a conventional, digital system, these new devices could potentially function more like a network of neurons.

"Computers are very impressive in many ways, but they're not equal to the mind," said Mark Hersam, the Bette and Neison Harris Chair in Teaching Excellence in Northwestern University's McCormick School of Engineering. "Neurons can achieve very complicated computation with very low power consumption compared to a digital computer."

A team of Northwestern researchers, including Hersam, has accomplished a new step forward in electronics that could bring brain-like computing closer to reality. The team's work advances memory resistors, or "memristors," which are resistors in a circuit that "remember" how much current has flowed through them.

The research is described in the April 6 issue of *Nature Nanotechnology*. Tobin Marks, the Vladimir N. Ipatieff Professor of Catalytic Chemistry, and Lincoln Lauhon, professor of materials science and engineering, are also authors on the paper. Vinod Sangwan, a postdoctoral fellow co-advised by Hersam, Marks, and Lauhon, served as first author. The remaining co-authors--Deep Jariwala, In Soo Kim, and Kan-Sheng Chen--are members of the Hersam, Marks, and/or Lauhon research groups.

"Memristors could be used as a memory element in an integrated circuit or computer," Hersam said. "Unlike other memories that exist today in modern electronics, memristors are stable and remember their state even if you lose power."

Current computers use random access memory (RAM), which moves very quickly as a user works but does not retain unsaved data if power is lost. Flash drives, on the other hand, store information when they are not powered but work much slower. Memristors could provide a memory that is the best of both worlds: fast and reliable. But there's a problem: memristors are two-terminal electronic devices, which can only control one voltage channel. Hersam wanted to transform it into a three-terminal device, allowing it to be used in more complex electronic circuits and systems.

Hersam and his team met this challenge by using single-layer molybdenum disulfide (MoS2), an atomically thin, two-dimensional nanomaterial semiconductor. Much like the way fibers are arranged in wood, atoms are arranged in a certain direction--called "grains"--within a material. The sheet of MoS2 that Hersam used has a well-defined grain boundary, which is the interface where two different grains come together.

"Because the atoms are not in the same orientation, there are unsatisfied chemical bonds at that interface," Hersam explained. "These grain boundaries influence the flow of current, so they can serve as a means of tuning resistance."

When a large electric field is applied, the grain boundary literally moves, causing a change in resistance. By using MoS2 with this grain boundary defect instead of the typical metal-oxide-metal memristor structure, the team presented a novel three-terminal memristive device that is widely tunable with a gate electrode.

"With a memristor that can be tuned with a third electrode, we have the possibility to realize a function you could not previously achieve," Hersam said. "A three-terminal memristor has been proposed as a means of realizing brain-like computing. We are now actively exploring this possibility in the laboratory."

AJAY KUMAR

BE – IT

HOW TO DISABLE YOUR WEBCAM (AND WHY YOU SHOULD) …

Once a concern that was the province of the paranoid, years' worth of reports and revelations have made it readily apparent that people really can (and do) spy on you through your webcam. Read on as we discuss why you should disable or cover your webcam, how you can do so, and review some handy products that can help make the job simple.

TLDR version: Script-kiddie hackers and teenagers can, and do, use easily accessible tools and phishing techniques to hijack webcams of unsuspecting people, often who they know, and watch them through their camera. They can store images and videos of people in compromising situations in their bedrooms, and many of these images and videos are uploaded to shady websites.

If you have kids, you should strongly consider reading the entirety of this article and implementing something to stop their webcams from being on all the time (or ever).

IS WEBCAM SPYING REALLY A THREAT?

In early 2015, a group known as BlackShades was broken up after it was discovered that the software they sold for $40 a pop had been used to give millions of purchasers remote access (including webcam access) to victims computers; that's hardly a new Ten years ago the idea that people, be they government agents, hackers, or just law-breaking voyeurs, could actively spy on you through your computer's webcam would be the considered the ramblings of a paranoid conspiracy theorist at worst or a hypervigilant privacy advocate at best. A slew of news stories

over the intervening years, however, have revealed that what was once considered paranoia is now an uncomfortable reality.

In 2009, a student sued his school when he discovered his school-provided laptop was secretly photographing him (the ensuing legal investigation revealed that the school had collected 56,000 photographs of students without their knowledge or consent). In 2013, researchers demonstrated that they could activate the webcam on MacBooks without the indicator light turning on, something previously considered impossible. A former FBI agent confirmed that not only was this possible but that they'd been doing it for years.

In 2013, courtesy of the documents leaked by Edward Snowden, we learned that the NSA had successful programs they used to gain backdoor access to the cameras on iPhones and Blackberries. In 2014, again courtesy of the Snowden leaks, we learned that the NSA has a host of tools at its disposal to remotely monitor users like "Gumfish": a malware tool that allows for remote video monitoring via your webcamtrick though as old programs like Back Orifice were used in the same fashion back in the 1990s.

IT'S NOT JUST THE NSA

We want to emphasize the whole "hardly a new trick" bit and the ease with which even marginally skilled malicious users can gain access to your computer. This long-form article over at ArsTechnica, Meet The Men Who Spy On Women Through Their Webcams, is an unsettling account that really drives home that the majority of people doing the spying aren't government agents but low-tier hackers that use simple phishing tricks and malicious websites to net thousands upon thousands of computers and then, for little more than their own amusement in most cases, use simple tools to catalog and monitor all the devices they have access to.

Call them Remote Access Tools (RATs), call them Trojans, call them malware, regardless of the name there are clear and well documented examples in the wild that show you simply cannot trust that your webcam is only active when you're snapping selfies or Skyping. Further, you can't even trust the indicator light as the camera can be active without the light enabled.

So the short of it is: yes, webcam spying is a real threat. When everyone from the spooks at the NSA to the kid next door has access to tools that can turn a webcam against its owner then the threat is legitimate.

WHAT SHOULD I DO?

You should, no questions asked, disable or obscure your computer's webcam. There is no good reason, especially in light of the numerous documented cases of webcam spying, to leave an insecure recording device permanently accessible and/or active on your computer.

Given the ease with which you can, in most cases, permanently disable or remove a webcam if you don't use it (or use it infrequently) and the ease with which you can temporarily modify it to obscure the lens if you are a frequent webcam user, it makes little sense not to do so.

DISABLE IT IN THE BIOS

This option is only viable for laptops with integrated webcams (and those rare all-in-one desktop models that also sport integrated webcams in the monitor frame). In order to disable the webcam via the BIOS, the BIOS and the hardware must support such a function.

Reboot your computer and enter into the BIOS (follow the onscreen instructions, typically you access the BIOS by pressing the F2 key, the DEL key, or a function key combination of some sort). Look through the BIOS options for an entry labeled something like "webcam," "integrated camera," or "CMOS camera." These entries will typically have a simple toggle like enable/disable or lock/unlock. Disable or lock the hardware to turn off your webcam.

Unfortunately the BIOS solution is relatively rare and typically found on computers from vendors with heavy institutional sales. Dell and Lenovo laptops, for example, commonly ship with this feature in the BIOS because their corporate buyers want the ability to lock/disable the webcam. With other vendors (and even within computer lines from the aforementioned vendors) it's hit or miss. Be forewarned that disabling the webcam typically disables the microphone too as in most laptops the camera and microphone module are on the same small expansion board. This is obviously a benefit (from a privacy standpoint) but you should be aware of it so you're not left wondering why your mic is dead.

ANKITA CHOWDHURY

TE-IT

WEARABLE TECHNOLOGY CAN HELP WITH PUBLIC SPEAKING

Speaking in public is the top fear for many people. Now, researchers from the Human-Computer Interaction Group at the University of Rochester have developed an intelligent user interface for "smart glasses" that gives real-time feedback to the speaker on volume modulation and speaking rate, while being minimally distracting.

The Rochester team describes the system, which they have called Rhema after the Greek word for "utterance," in a paper that will be presented on Tuesday, March 31 at the Association for Computer Machinery's Intelligent User Interfaces (IUI) conference in Atlanta.

Smart glasses with Rhema installed can record a speaker, transmit the audio to a server to automatically analyze the volume and speaking rate, and then present the data to the speaker in real time. This feedback allows a speaker to adjust the volume and speaking rate or continue as before.

Ehsan Hoque, assistant professor of computer science and senior author of the paper, used the system himself while giving lectures last term. "My wife always tells me that I end up speaking too softly," he says. "Rhema reminded me to keep my volume up. It was a good experience." He feels the practice has helped him become more aware of his volume, even when he is not wearing the smart glasses.

In the article, Hoque and his students M. IftekharTanveer and Emy Lin explain that providing feedback in real-time during a speech presents some challenges. "One challenge is to keep the speakers informed about their speaking performance without distracting them from their speech," they write. "A significant enough distraction can introduce unnatural behaviors, such as stuttering or awkward pausing. Secondly, the head mounted display is positioned near the eye, which might cause inadvertent attention shifts."

Tanveer, the lead author of the paper, explains that overcoming these challenges was their focus. To do this, they tested the system with a group of 30 native English speakers using Google Glasses. They evaluated different options of delivering the feedback. They experimented with using different colors (like a traffic light system), words and graphs, and no feedback at all (control). They also tried having a continuous slowly changing display and a sparse feedback system, by which the speaker sees nothing on the glasses for most of the time and then just sees feedback for a few seconds. After user-testing, delivering feedback in every 20 seconds in the form of words ("louder,""slower," nothing if speaker is doing a good job, etc.) was deemed the most successful by most of the test users.

The researchers also highlight that the users, overall, felt it helped them improve their delivery compared to the users who received continuous feedback and no feedback at all. They also addressed the system from the point of view of the audience and enlisted 10 Mechanical Turk workers.

"We wanted to check if the speaker looking at the feedback appearing on the glasses would be distracting to the audience," Hoque said. "We also wanted the audience to rate if the person appeared spontaneous, paused too much, used too many filler words and maintained good eye contact under the three conditions: word feedback, continuous feedback, and no feedback."

However, there was no statistically significant difference among the three groups on eye contact, use of filler words, being distracted, and appearing stiff, judged by the Mechanical Turk workers. As part of their future work, the researchers want to test their system with members of Toastmasters International as a more knowledgeable audience.

The researchers also believe that live feedback displayed in a private and non-intrusive manner could also be useful for people with social difficulties (e.g., Asperger syndrome), and even for people working in customer service.

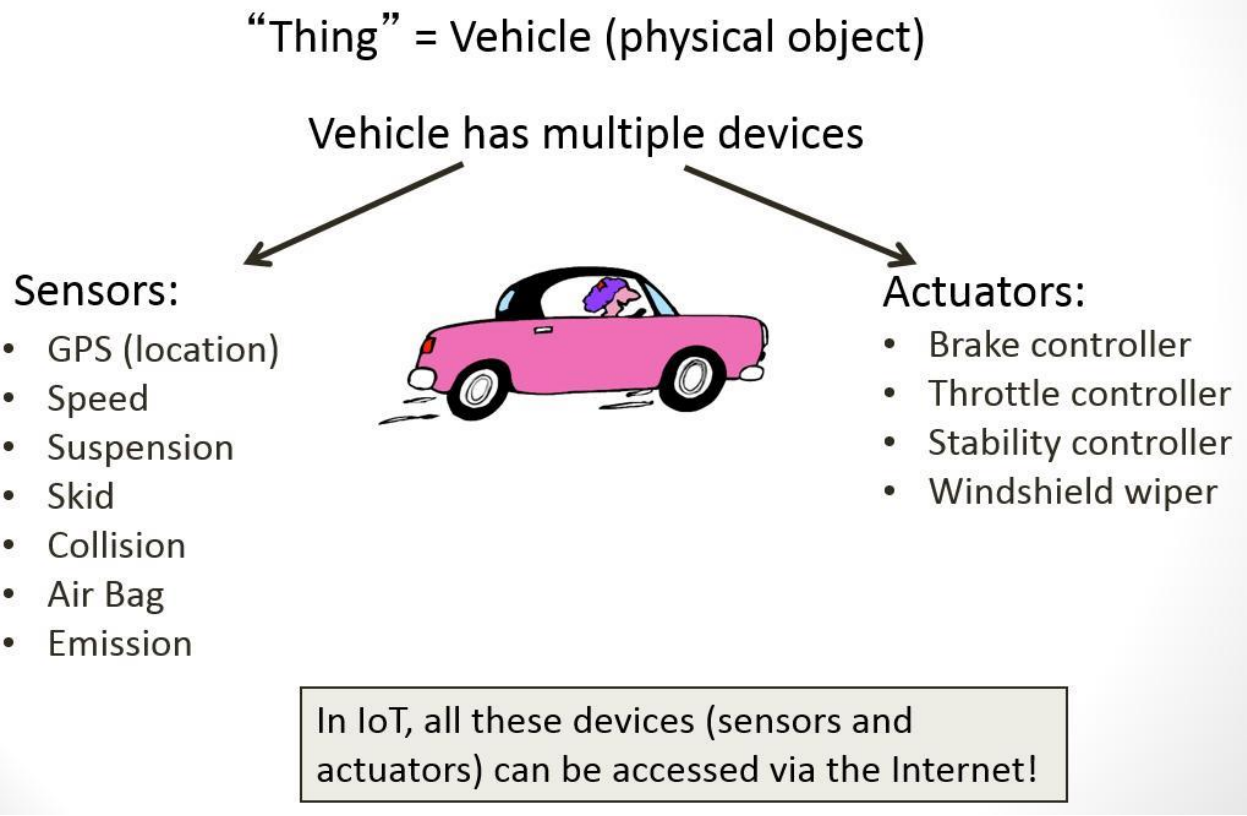
SOUMYA IYENGER

BE – IT

WHAT MAKES UP THE INTERNET OF THINGS?

Most definitions of the Internet of Things include physical objects or devices (also called "things") that can sense and/or affect the physical environment, as shown in Figure 1. By 2020, it is expected that the IoT will comprise 50 billion devices, as shown in Figure 3. The IoT also includes virtual objects, such as electronic tickets, agendas, books, and wallets.

The Internet of Things also includes people – this is particularly important in areas such as home automation, where humans can control the environment via mobile applications. Through services, such as cloud services, massive volumes of data ("big data") are being processed and turned into valuable information, innovative applications are built and run, and business processes are being optimized by integrating device data, as shown below.



Also needs IoT Platforms – the type of middleware that is used to connect the IoT components (objects, people, services, etc.) to the IoT. The IoT platforms provide numerous functions, such as access to devices, ensuring the proper installation and behavior of the device, data analytics, and interoperable connection to the local network, cloud, or other devices. Finally, all of the components in an IoT environment should be tied together by networks through various wireless and wireline technologies, standards, and protocols to provide pervasive connectivity.

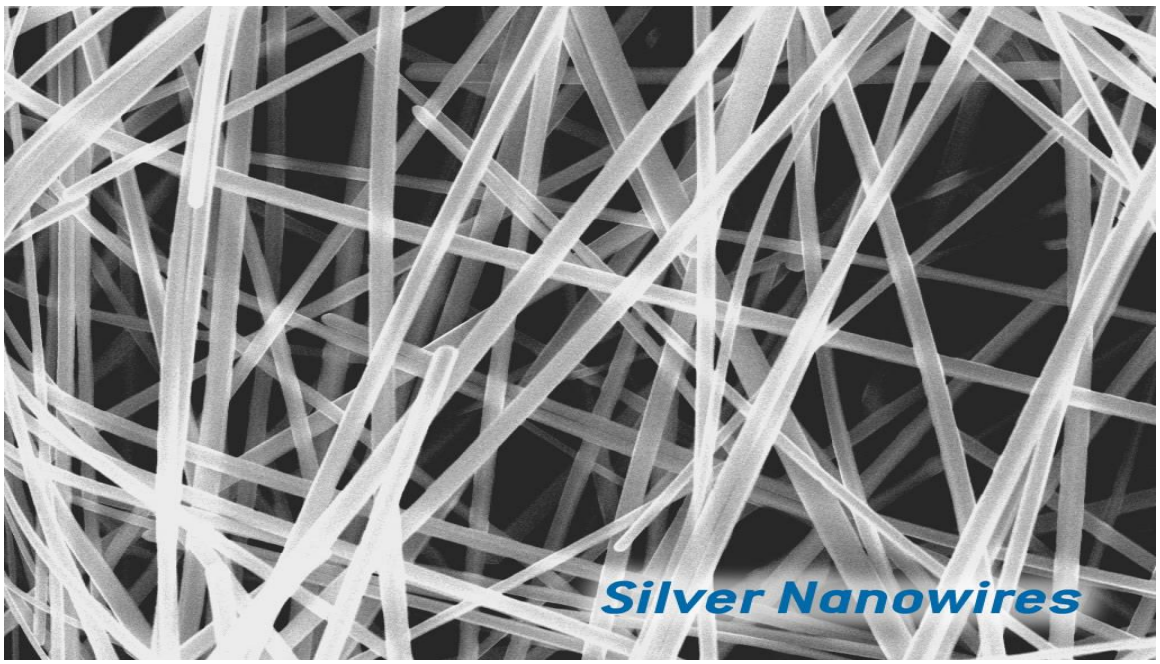
IoT Components	Description
Physical Objects:	Things
Sensors	Sense the physical environment
Actuators	Affect the physical environment
Virtual Objects	Electronic tickets, Agendas, Books, Wallets
People	Ex.: Humans can control the environment via mobile apps
Services	Ex.: Cloud services – can be used to: • Process big data and turn it into valuable information • Build and run innovative applications • Optimize business processes by integrating device data.
Platforms	Type of middleware used to connect IoT components (objects, people, services, etc.) to IoT. Provide numerous functions: • Access to devices • Ensuring proper installation/behavior of device • Data analytics • Interoperable connection to local network, cloud or other devices.
Networks	IoT components are tied together by networks, using various wireless and wireline technologies, standards, and protocols to provide pervasive connectivity.

Looking at the current IoT landscape, among "the good" are the standards efforts (including architectural and platform reference implementations), the growing number of available products, and the numerous potential benefits. Among "the bad" are the overlapping IoT standards efforts, apparent incompatibility of devices with proprietary technologies, and multiple complex security challenges.

ADITYA JADHAV

TE - IT

HOW SILVER NANOWIRE TECHNOLOGY IS IMPROVING TOUCHSCREEN CAPABILITY



Demand for new electronic applications is driving opportunities for transparent conductors—and the need for a cost-effective material that conforms to bends and curves, is flexible, and foldable.

Using silver nanowire coatings is one possibility being explored to achieve those curves. Silver nanowires have significantly higher optical and electrical conductivity than currently used materials such as indium tin oxide (ITO) and other transparent conductors.

Applying it to transparent conductors based on silver nanowires, manufacturers can turn strange and varied surfaces— even bendable, transparent surfaces like a piece of plastic—into touch-sensitive surfaces for computing device human interfaces.

EVOLVING TOUCHSCREEN REQUIREMENTS

Currently, device makers prefer conductivity below 100/sq, making their touchscreens more responsive and noticeably improving the user's experience.

For larger-area touchscreens such as 20-inch monitors, higher conductivity is essential for faster response times and detecting 10-finger touch. In mobile devices, including laptops and

smartphones, film-based transparent conductors enable significantly thinner, lighter, and shatterproof touchscreens.

Flexible displays demand transparent conductors that can be bent or rolled. Most importantly, transparent conductor prices must be low enough to enable mass production and mass adoption of touch in new products.

Silver nanowires are being adopted as the transparent-conductor of choice by leading industry heavyweights including Hitachi, LG, TPK, Nissha, 3M, Okura, and many others.

Silver nanowire conductors also deliver improved light transmission and can be patterned using lasers where there are no consumables (like etchants) thus reducing processing costs.

Further manufacturing advantages includes capital equipment to make silver nanowire-based transparent conductors at a fraction of what it costs for ITO. Silver nanowires are available in cost-effective, high production volumes. And true single-layer sensors are possible with silver nanowires that reduce total material used and further lowers costs.

THE FLEXIBILITY FACTOR

In customer tests, silver-nanowire-coated films withstood bending greater than 100,000 turns around a 3mm radius, clearly demonstrating their fit for flexible electronic devices. It enables flexible/transparent devices, whereas the incumbent ceramic material is brittle and will break.

Additionally, silver nanowires simplify touchscreen manufacturing processes and improve end-product performance in consumer electronics designs beyond legacy technologies. There isn't a downside. Overall, silver-nanowire-based touchscreen costs range from slightly less to significantly less than the cost of equivalent ITO, film-based solutions. The material is cost-effectively accelerating the transition to flexible and wearable devices.

LOOKING AHEAD

This hot sector potential is reinforced by IDTechEx, which noted that wearable technology requires new form factors, and printed, organic and flexible electronics can lead to products that can be priced to generate healthy margins.

Flexible OLED display shipments alone are expected to reach 86.2 million units globally in 2020, up from only sample volumes in 2015, according to a recent IDTechEx report entitled “OLED Display Forecast 2015-2025: the Rise of Plastic and Flexible Displays“. The report projects that market revenue for flexible displays will grow to $7.3 billion during the same five-year period.

To bring wearable technology to the forefront, the human interface must radically evolve. Brittle glass is out and flexible film is in.

Flexibility provides enhanced portability and durability, and allows virtually unlimited design freedom. Flexible displays essentially equate to superior ergonomics. Imagine unbreakable phone screens that flex instead of shattering when dropped. Consider folding a seven-inch tablet so it slips into your pocket. How about a display that wraps around your arm, or a large public display wrapping around a pillar or a building?

Moving toward products like these creates increased demand for flexible, bendable, and roll able touchscreens. As more product designers become aware of silver nanowire-based touch displays, we'll be seeing great new products.

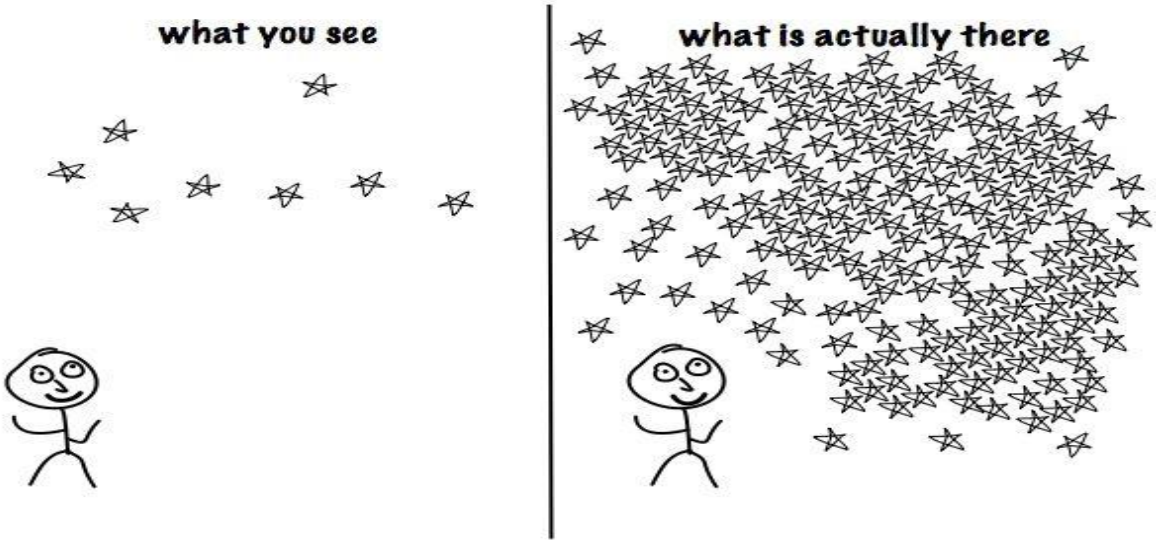
BOOSTING USER EXPERIENCE

As expectations for low-cost, high-performance touchscreens increase so does demand for higher quality touch screens. Meeting today’s advanced standards means touchscreens must be thin, light, visible in various ambient light conditions, highly responsive, and of course low-cost. Fast-responding transparent touchscreens are essential to the desired user experience. This result can only be achieved with highly transparent conductors not visible to the eye. An essential enabler of these important benefits is silver nanowire conductor technology.

VENUVANSHI BHUJBAL

BE - IT

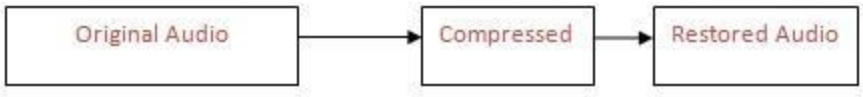
MP3 FORMAT: UNDERSTANDING THE BASICS OF DIGITAL MUSIC



In today's world, the word MP3 has become synonymous with music. Almost everyone has experienced MP3 in some way – be it through listening to your favourite songs on your music player or phone, the internet, a podcast or something similar. MP3 has revolutionized the digital music world on its own and even though it's been around for quite some time, the MP3 still remains the most popular form of music used across the globe.

Now, even though it's something that we use on a daily basis, have you ever wondered **how it works**? Well, this article aims to inform you about that as well as the basic principles involved in the process.

But first, **what exactly is MP3**? The MP3 format is basically an audio-specific format which uses a compression system to reduce the size of music files. **MP3 stands for MPEG Phase 1 Layer 3**, where MPEG refers to **Motion Picture Experts Group** which is a family of standards for displaying video and audio using lossy compression. A 'lossy' compression implies that during the compression process, some of the audio data was lost which leads to the creation of a file not identical to its original. A simple schematic of the lossy compression algorithm is shown below:



Layer 3 is one of three coding schemes for the compression of audio data. It uses perceptual audio coding and psychoacoustic compression to remove all unnecessary information in the

signals. It also adds a MDCT (Modified Discrete Cosine Transform) that implements a filter bank, increasing the frequency resolution 18 times higher than that of layer 2. This result in a file reduced in size with minimal audio degradation. MP3 now uses the ID3 tagging system of an audio file with details associated with its ownership, production and contents - a system which can be used to catalogue and manage collections of MP3 files.

Now, let's go back – who created the MP3 and what was the need for it? MP3 technology was developed between 1987 and 1991 by engineers at the German company FraunhoferGesellschaft as an attempt to reduce digital audio file size with the minimum degradation of perceived audio quality. The inventors for the MP3 patent are Bernhard Grill, Karl-Heinz Brandenburg, Thomas Sporer, Bernd Kurten, and Ernst Eberlein.

Uncompressed audio files are rather large, as sound is very complex and the translation of it into a digital format that a computer can understand requires a lot of data. MP3 works to make file sizes smaller by using what is called psychoacoustic models. In this model, the audio signals that most people would not hear because it is too low or too high are eliminated. By doing this, file sizes can be greatly reduced. A 128 Kbit/s MP3 file is about $1/11^{th}$ the size of the corresponding file on an uncompressed CD. This smaller size enables faster delivery via the internet, and easier sharing and portability, as well as its reduced mass storage requirements.

PRINCIPLE – COMPRESSION ALGORITHM AND PSYCHOACOUSTICS

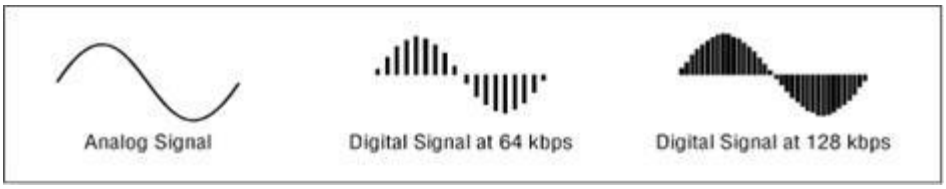
Two kinds of compression methods are used for reduction of music files in MP3. First, it filters out what is inaudible to the human ear (if the signal frequencies are too high or too low) and next it works on encoding the remaining data via more traditional means (like the 'zip' compression method) to further compress the files. This compression technique results in loss of audio signal data, hence it is termed as lossy compression.

Consider these two scenarios: 1. you hear two similar notes one after the other, very close together in time; the result - your brain may perceive only one of them. 2. You hear two different sounds but one is much louder than the other; the result - your brain may never perceive the quieter signal. The study of these auditory phenomena is called psychoacoustics. MP3 coding takes advantage of this psychoacoustic phenomenon to make changes to the signals, and thus reduces the amount of information needed to express it in digital form, decreasing its file size considerably.

MP3 format is often termed as a perceptual codec as it mathematically describes the limitations of auditory perception. The basic principle of any perceptual codec is that there's little point in storing information that can't be perceived by humans. MP3 encoding tools analyze incoming source signal, break it down into mathematical patterns, and compare these patterns to psychoacoustic models stored in the encoder itself. The encoder can then throw away most of the data that doesn't match the stored models, while retaining that which matches.

PROCESS DESCRIPTION

The key to audio compression in MP3 lies in the bit rate – the number of bits per second encoded in the audio file. If the bit rate is low, the encoder will discard more data and vice versa. The basic working follows that an MP3 encoder splits the signal into 22 frequency bands and then process each band separately for storage. These signals are then decoded and recombined for playback.



As shown above, if the bitrate is high, the signal is effectively conveyed with better resolution but higher file size. In case of smaller bitrate, the size is reduced but the audio resolution is changed accordingly.

Let’s break down the MP3 building process:

- The first step is to divide the source audio into components called 'frames', which individually contains about a fraction of a second’s audio data. This happens every 26 ms or .026 seconds, i.e. creating approximately 38 frames per second.
- The signal is analyzed to determine the distribution of bits for the best possible account of the audio on the entire spectrum. This involves splitting the signal into different bands based on frequency.
- The audio in these frames is then compressed to a target number of bits using psychoacoustic modelling. The bitrate is used to calculate the number of bits that can be allocated to each frame and hence the amount of audio data to be stored is decided. The band frequencies of the signal are compared to the reference models in the encoder itself, and the ones that do not match are discarded.
- The remaining data is compressed to shrink the space for redundancies via traditional means and Huffman coding.

- The collection of frames is assembled into a serial bit-stream, with header information preceding each data frame. The headers contain instructional "meta-data" specific to that frame. Each frame header contains 32 bits, comprised of a synchronisation reference number and various other identifiers of the frame's contents (bitrate, sample rate, etc.). The header is then followed by the frame's audio data. This series of frames constitutes the standard MP3 file.

AKSHAYSARDA

BE – IT

EXPECTIONS FROM APPLE'S SPRING FORWARD EVENT

What a rocking enthusiasm we have seen in MWC 2015 (Mobile World Congress 2015). If you are thinking that after MWC there is no new news in tech world then you are wrong. Most of the tech companies showed there upcoming plans in MWC 2015.

When MWC 2015 is started everyone wanted to know about the future plans of APPLE in coming year. Absence of Apple in MWC 2015 made many Apple lovers bit nervous. There is a good news to Apple lovers. On coming Monday March 9 Apple is going to hold "Spring Forward" event to represent companies' new strategy and plans with Apple's new Devices and Gadgets.

HOW CAN YOU WATCH IT?

Mostly Apple's events are live-streamed on Apple's Website. If you are unable to watch it then you have to wait until its get aired on YouTube. If you are OSX and iOS users the it will be easy for you to watch "Spring forward" without any disturbances. Key-points on which Apple is going to focus: Apple Watch.

- Wear devices
- New applications for Apple Watch
- New 12-inch MacBook Air with Retina display
- The 12-inch iPad Pro
- New version of iOS – 8.2
- New music streaming service.

In 2015, its not new thing that wearable electronic devices will be tech-centric as compared to mobile devices. After Samsung's Gear watch, Sony's smart watch, LG's G watch , Motorola's 360 watch and Microsoft's watch band, everyone is waiting for the Apple's watch which is pretty impressive.

WHY APPLE WATCH IS SO ANTICIPATED?

As like as other products of Apple, This watch also said to be offer premium colour and material choices. There will be lot of customization options like which colour and material will be suitable for Apple Watch? Lot of customization will be there if you are going to buy Apple Watch and lot of option range such as Glass finishing , metal finishing and straps like rubber , leather and steel, etc. And as like a trend every company used to publish gold edition gadget of their flagship model. So, rumour is that tomorrow Apple can launch watch covered with a golden sapphire glass. Another key-point is functionality of the wearable device. Functionality of wearable device depends on the number of supported applications available in the market. Today's time Android has number of supported applications on Play Store. Rumours is that tomorrow Apple is going to show us new environment where large number of dedicated applications will be available for Apple's wearable devices. It helps to enhance the experience of user. Mainly this topic is going to major key-point for Apple and I am pretty sure about this. According to Apple's insiders tomorrow Apple is going to launch near about 100000 apps for its wearable eco-system.

CHAITANYA AMBARDEKAR

TE – IT

6 STEPS TO PREVENT YOUR BUSINESS FROM BEING HACKED

Cyber security is essential for business owners in 2015. There have been numerous security breaches of major companies just in the last few months, including Anthem Insurance Agency, Sony, and Target. Both public and private businesses alike face the threat of hackers invading their data files and unearthing the personal information of millions of people as well as the possibility of disabling or limiting services to clients.

This is a very serious and overwhelming problem, but luckily, it can be combated by employing a few preemptive strategies in your security plan.

1. PREPARE YOUR EMPLOYEES.

Anthem suffered the most recent security breach this year when 80 million customers' names, e-mail addresses, and social security numbers were stolen by hackers. The initial breach appears to be caused by select employees responding to "phishing" e-mails, opening the gates for hackers to intercept the IT servers with malware.

Phishing e-mails often look legitimate, claiming to be from real companies or real employees from those companies, they are just a fraudulent means to extract information from people on the inside of the business.

Businesses need to train employees what these e-mails look like and how to address them. Simple tutorials on the subject would create more awareness and ultimately prevent a destructive breach in the future.

2. ALWAYS VERIFY.

Inform employees that if they receive a suspicious looking e-mail, do not respond, open any attachments, or click any links that may be embedded in the e-mail. Tell them to look up the number for the business the e-mail claims to be representing, and then call them directly.

Do not follow any information given in the fraudulent e-mail. If there is a link provided in the e-mail, type it into a search bar yourself, and do not follow the direct link to avoid a possible redirect.

If these steps have been taken and it is confirmed that the e-mail is trying to invade the computer systems of the company, inform the IT department or the head of cyber security immediately. The quicker these people find out the easier it will be to prevent a major information leak.

3. CREATE MORE LAYERS OF SECURITY PROTOCOL.

Hackers often access sensitive information by first invading the login accounts of security cleared personnel. To prevent this method of intrusion, create multiple levels of personal verification for users to access sensitive information.

Create algorithms that change pass codes to privileged information every day or every hour depending on the level of information sensitivity. Businesses will have to stay on top of the common protocol for servers and review access to detect suspicious logins. Always be aware of any unusual access and act immediately to fix any weak links in your security system.

4. ENCRYPT ALL OF YOUR FILES.

It seems like something simple, but Anthem revealed that the records that the millions of records that were hacked were not encrypted for safety. By using backup software, you can encrypt your data before it gets to a disk or storage device using software backup. By protecting your information at all stages of transfer, you minimize the chance of any breach interference.

Any information that travels across a wireless network are highly susceptible, so utilize a VPN (virtual private network) when working accessing any important information. It’s even advisable to encrypt portable devices in the event that they are stolen.

5. DON'T JUST CHECK YOUR OWN SECURITY; CHECK YOUR PARTNERS' TOO.

Although your security protocols may be top-notch and tightly monitored, it doesn't mean that the businesses you work with have the same sense of quality control. Interacting with third party vendors or financial institutions that have inadequate protection can also open your business for security breaches. Before continuing business with different companies, ask what measures they take to assure total protection from possible hacks.

6. STAY INFORMED, KEEP YOUR INFORMATION SAFE

The easiest preventative measure to avoid hacks is to stay informed and communicate with your colleagues and professionals in the field. Stay up to date on what potential scams are underway and what companies have failed to do to combat these threats.

Learn from other companies' mistakes and always check report hacking attempts to the Securities and Exchange Commission and the FBI. The more transparency businesses have with attempted hacks, the more government agencies can do to prevent more information being lost or the possibility of another devastating attack.

The main technique to preventing hacks into your business is awareness and education. Keep your employees informed and open to taking extra security measures in the face of possible information breaches.

The best thing you can do to protect your company's information is to be very familiar with everyday proceedings and immediately recognize when something is out of the ordinary. You can never do too much to protect the information for your employees, your customers, and yourself.

MEENAKSHI RATHOD

BE – IT

USB TYPE-C EXPLAINED: WHAT IT IS AND WHY YOU'LL WANT IT

Apple's new MacBook has a single USB Type-C port, but this isn't an Apple-only standard. This is a new USB standard, and — given time — it'll spread to everything that currently uses an older, larger USB connector.USB Type-C is closely intertwined with other new standards, like USB 3.1 for faster speeds and USB Power Delivery for improved power-delivery over USB connections.

TYPE-C IS A NEW CONNECTOR SHAPE

USB Type-C is a new, tiny physical connector. The connector itself can support various exciting new USB standard like USB 3.1 and USB power delivery (USB PD).

The standard USB connector you're most familiar with is USB Type-A. Even as we've moved from USB 1 to USB 2 and on to modern USB 3 devices, that connector has stayed the same. It's as massive as ever, and it only plugs in one way — so you have to make sure it's oriented correctly when you plug it in.

But other devices wanted to use USB, too! Those massive USB ports won't fit on smartphones, digital cameras, game controllers, and all the other devices out there you might want to plug in via USB. So many other shapes of connector were born, including "micro" and "mini" connectors.

This collection of differently shaped connectors for different-size devices is coming to a close. USB Type-C is a new connector standard that's very small. It's about a third the size of an old USB Type-A plug. This is a single connector standard that every device should be able to use. You'll just need a single cable, whether you're connecting an external hard drive to your laptop or charging your smartphone from a USB charger. That one tiny connector can be small and fit into a mobile device, or be the powerful port you use to connect all the peripherals to your laptop. The cable itself has USB Type-C connectors at both ends — it's all one connector.

Yes, this is many awesome things at once. Not only is it reversible, it's a single USB connector shape all devices should adopt. No more messes of different USB cables with different connector shapes for all the various devices you want, and no more massive ports taking up an unnecessary amount of room on ever-thinner devices.

USB Type-C ports can support a variety of different protocols using "alternate modes," which allows you to have adapters that can output HDMI, VGA, DisplayPort, or other types of connections from that single USB port, for example. Apple's USB-C Digital Multiport Adapter looks like a good example of this in action, offering an adapter that allows you to connect an HDMI or VGA output, larger USB Type-A connector, and smaller USB Type-C connector via a single port. The mess of USB, HDMI, DisplayPort, VGA, and power ports on typical laptops can be streamlined into a single type of port.

USB POWER DELIVERY

HTG Explains: Can You Use Any Charger With Any Device?

Every device — smartphone, tablet, e-Reader, laptop — seems to come with its own charger. But do you really need it?

The USB PD specification is also closely intertwined with USB Type-C. Currently, smartphones, tablets, and other mobile devices often use a USB connection to charge. A USB 2.0 connection provides up to 2.5 watts of power — that'll charge your phone, but that's about it. A laptop might require up to 60 watts, for example.

The USB Power Delivery specification ups this power delivery to 100 watts. It's bi-directional, so a device can either send or receive power. And this power can be transferred at the same time the device is transmitting data across the connection. Apple's new MacBook and Google's new Chromebook Pixel both use their USB Type-C ports as their charging ports. This could spell the end of all those proprietary laptop charging cables, with everything charging via a standard USB connection. You could charge your laptop from one of those portable battery packs you charge your smartphones and other portable devices from today. You could plug your laptop into an external display connected to a power cable, and that external display would charge your laptop as you used it as an external display — all via the one little USB Type-C connection.

To use this, the device and the cable have to support USB Power Delivery. Just having a USB Type-C connection doesn't necessarily mean they do.

USB TYPE-C AND USB 3.1

USB 2.0 vs. USB 3.0: Should You Upgrade Your Flash Drives?

New computers have now been coming with USB 3.0 ports for years. But just how much faster is USB 3.0?

USB 3.1 is a new USB standard. USB 3‘s theoretical bandwidth is 5 Gbps, while USB 3.1’s is 10 Gbps. That’s double the bandwidth, as fast as a first-generation Thunderbolt connector.

USB Type-C isn’t the same thing as USB 3.1. USB Type-C is just a connector shape, and the underlying technology could just be USB 2 or USB 3.0. In fact, Nokia’s N1 Android tablet uses a USB Type-C connector, but underneath it’s all USB 2.0 — not even USB 3.0. However, these technologies are closely related.

BACKWARD COMPATIBILITY

The physical USB Type-C connector isn’t backwards compatible, but the underlying USB standard is. You can’t plug older USB devices into a modern, tiny USB Type-C port, nor can you connect a USB Type-C connector into an older, larger USB port. But that doesn’t mean you have to discard all your old peripherals. USB 3.1 is still backwards-compatible with older versions of USB, so you just need a physical adapter with a USB Type-C connector on one and a larger, older-style USB port on the other. You can then plug your older devices directly into a USB Type-C port.

Realistically, many computers will have both USB Type-C ports and larger USB Type-A ports for the immediate future — like Google’s Chromebook Pixel. You’ll be able to slowly transition from your old devices, getting new peripherals with USB Type-C connectors. Even if you get a computer with only USB Type-C ports, like Apple’s new MacBook, adapters and hubs will fill the gap.

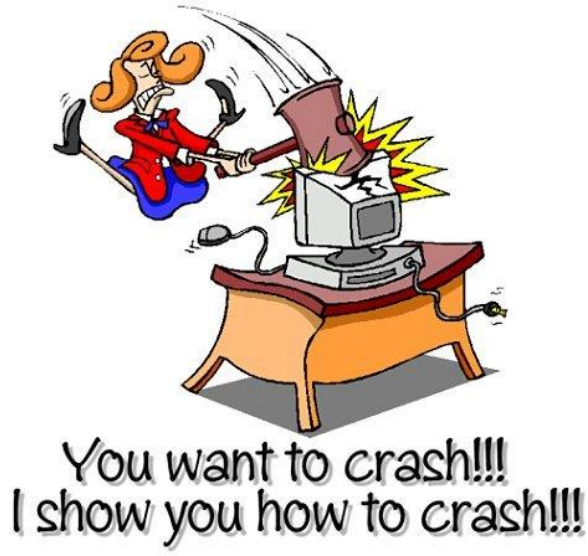
USB Type-C is a worthy upgrade. It’s making waves on the new MacBook, but it’s not an Apple-only technology and it will shortly be appearing in devices from practically everyone. Whatever you think of Apple, this time around they’re pushing hard behind a new standard that everyone can adopt.

USB Type-C may even replace the Lightning connector on Apple’s iPhones and iPads one day — Lightning doesn’t have many advantages over USB Type-C besides being a proprietary standard Apple can charge licensing fees for.

ANKITA CHOWDHURY

TE-IT

THE COMPUTER THAT NEVER CRASHES



A revolutionary new computer based on the apparent chaos of nature can reprogram itself if it finds a fault OUT of chaos, comes order. A computer that mimics the apparent randomness found in nature can instantly recover from crashes by repairing corrupted data.

Dubbed a "systemic" computer, the self-repairing machine now operating at University College London (UCL) could keep mission-critical systems working. For instance, it could allow drones to reprogram themselves to cope with combat damage, or help create more realistic models of the human brain.

Everyday computers are ill suited to modelling natural processes such as how neurons work or how bees swarm. This is because they plod along sequentially, executing one instruction at a time. "Nature isn't like that," says UCL computer scientist Peter Bentley. "Its processes are distributed, decentralised and probabilistic. And they are fault tolerant, able to heal themselves. A computer should be able to do that."

Today's computers work steadily through a list of instructions: one is fetched from the memory and executed, then the result of the computation is stashed in memory. That is then repeated – all under the control of a sequential timer called a program counter. While the method is great for number-crunching, it doesn't lend itself to simultaneous operations. "Even when it feels like your computer is running all your software at the same time, it is just pretending to do that, flicking its attention very quickly between each program," Bentley says.

He and UCL's Christos Sakellariou have created a computer in which data is married up with instructions on what to do with it. For example, it links the temperature outside with

what to do if it's too hot. It then divides the results up into pools of digital entities called "systems".

Each system has a memory containing context-sensitive data that means it can only interact with other, similar systems. Rather than using a program counter, the systems are executed at times chosen by a pseudorandom number generator, designed to mimic nature's randomness. The systems carry out their instructions simultaneously, with no one system taking precedence over the others, says Bentley. "The pool of systems interact in parallel, and randomly, and the result of a computation simply emerges from those interactions," he says.

It doesn't sound like it should work, but it does. Bentley will tell a conference on evolvable systems in Singapore in April that it works much faster than expected.

Crucially, the systemic computer contains multiple copies of its instructions distributed across its many systems, so if one system becomes corrupted the computer can access another clean copy to repair its own code. And unlike conventional operating systems that crash when they can't access a bit of memory, the systemic computer carries on regardless because each individual system carries its own memory.

The pair is now working on teaching the computer to rewrite its own code in response to changes in its environment, through machine learning.

"It's interesting work," says Steve Furber at the University of Manchester, UK, who is developing a billion-neuron, brain-like computer called Spinnaker (see "Build yourself a brain"). Indeed, he could even help out the UCL team. "Spinnaker would be a good programmable platform for modelling much larger-scale systemic computing systems," he says.

ANUJ MORE

BE – IT

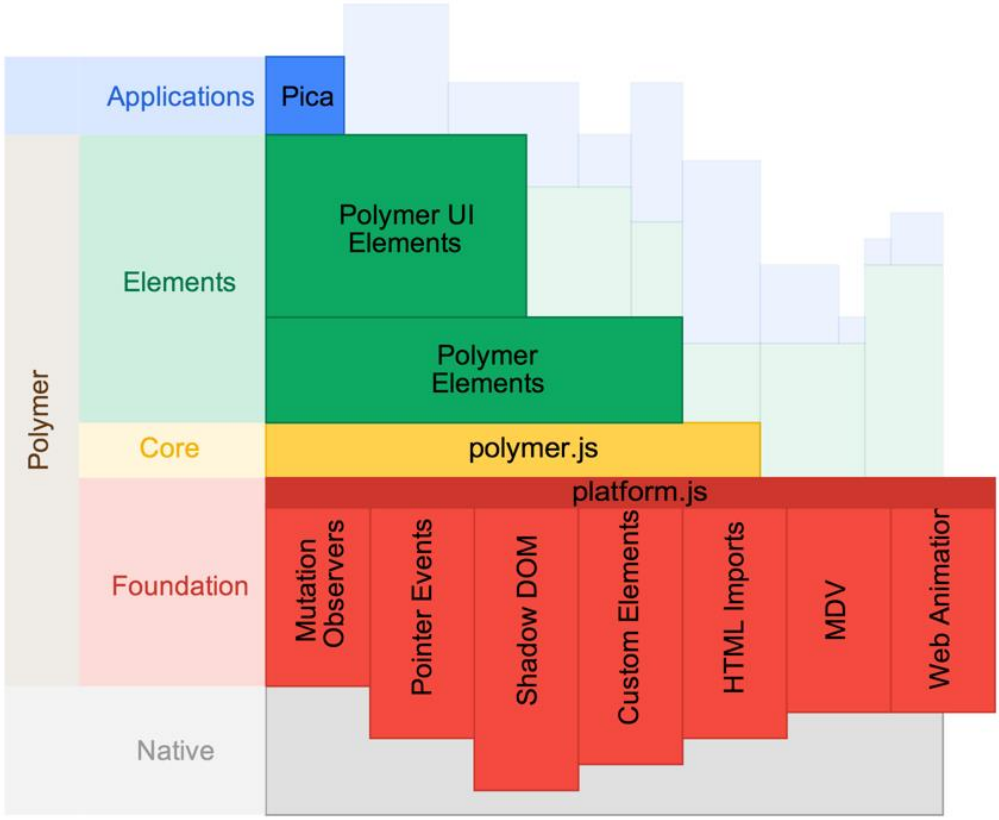
Polymer is a library for creating Web Components, which are a set of W3C standards and upcoming browser APIs for defining your own custom HTML elements. With the help of polyfills and sugar, it can create these custom elements and bring Web Component support to browsers that don't play nice with the standard just yet. Custom elements look like this:

<google-map lat="37.790" long="-122.390"></google-map>

They are very similar to Angular directives. The result would be a Google Map plugged directly into your webpage.

POLYMER ARCHITECTURE:

Polymer is a framework that aims to use (and show how to use) Web Components. It's foundation is Custom Elements (e.g. everything you build is a web component) and it evolves as the web evolves. To that end, we only support the latest version of the modern browsers.



Polymer's entire architecture stack

RED layer: We get tomorrow's web through a set of poly fills. Keep in mind, those libraries go away over time as browsers adopt the new APIs.

YELLOW layer: Sprinkle in some sugar with polymer.js. This layer is our opinion on how to use the spec'd APIs, together. It also adds things like data-binding, syntactic sugar, change watchers, published properties...We think these things are helpful for building web component-based apps.

GREEN: The comprehensive set of UI components (green layer) is still in progress. These will be web components that use all of the red + yellow layers.

HOW DOES POLYMER DIFFER FROM ANGULAR?

Angular is a complete framework for building web apps, whereas Polymer is a library for creating Web Components. Those components, however, can then be used to build a web app.

Angular has high-level APIs for things like services, routing, server communication and the like. Polymer, on the other hand, doesn't provide these things except as separate web components from their core library. Instead, it focuses on allowing you to create rich, powerful, reusable web components, which could be used to build web apps like those built with Angular. In the future, the lines could be blurred further as frameworks like Angular may leverage Web Components.

Even though Angular and Polymer aim to do different things, there is currently some overlap. Web components and Angular's element directives are very similar, and if there's a comparison to be made it should be between Polymer's Custom Elements and Angular's directives.

MRS. R. Y. TOTARE

ASSISTANT PROFESSOR, IT

Man is still the most EXTRAORDINARY COMPUTER of all.

-John F. Kennedy

Designed By: Rishikesh Jadhav

All India Shri Shivaji Memorial Society's

Intitute Of Inrormation Technology

IT Department

Kennedy Road, Pune-411001, Maharashtra , India
Ph. +91(202)26058877, Fax. +91(020)2605997
Email: aissmsioit@hotmail.com, Website: aissmsioit.org